

[Print](#) | [Close](#)**Patent Record View**

Wednesday, March 17 2010

**THOMSON INNOVATION**

Patent/Publication: EP1190526A1 METHODS AND ARRANGEMENTS FOR SECURE LINKING OF ENTITY AUTHENTICATION AND CIPHERING KEY GENERATION

**Bibliography****DWPI Title**

Communications systems method and arrangements for secure linking of entity authentication and ciphering key generation conducts entity authentication process using cryptography key when a cuphering offset value is generated

**Original Title**

METHODS AND ARRANGEMENTS FOR SECURE LINKING OF ENTITY AUTHENTICATION AND CIPHERING KEY GENERATION

**Assignee/Applicant**

Standardized: **ERICSSON TELEFON AB L M**

Original: Telefonaktiebolaget LM Ericsson (publ)

**Inventor**

SMEETS Ben

**Publication Date (Kind Code)**

2002-03-27 (A1)

**Application Number / Date**

EP2000943854A / 2000-06-21

**Priority Number / Date / Country**

US1999344387A / 1999-06-25 / US

US1999344387A / 1999-06-25 / US

EP2000943854A / 2000-06-21 / EP

WO2000EP5742A / 2000-06-21 / EP

**Abstract****Abstract**

Methods and arrangements are provided for use in communications systems that allow for secure communication sessions to be conducted over a communications link between at least two nodes (12', 16'). An entity authentication process is conducted using a cryptography key (70). During the authentication process, a ciphering offset (COF) value (50) is generated. Each node (12', 16') stores the COF value (50) and uses the COF value (50) to generate subsequent ciphering keys (70) that are employed to encrypt data transmitted between the nodes (12', 16'). As such, there is a logical relationship between the latest entity authentication process and subsequently generated ciphering keys (70). This increases security and can be used to reduce overhead processing/delays associated with repeating the link or entity authentication process. The methods and arrangements can be employed to enhance security in any communications system, including a mobile telecommunications system, such as, for example, a global system for mobile (GSM) communications system.

**French Abstract**

L'invention concerne des procédés et des dispositifs destinés à des systèmes de communication qui permettent le déroulement de sessions sécurisées via une liaison de communication entre au moins deux noeuds (12', 16'). Un processus d'authentification d'entité est exécuté à l'aide d'une clé de chiffrement (70). Pendant le processus d'authentification, une valeur de correction de chiffrement (COF) (50) est générée. Chaque noeud (12', 16') stocke la valeur COF (50) et utilise cette valeur COF (50) pour générer des clés de chiffrement consécutives (70) qui sont utilisées pour chiffrer des données transmises entre les noeuds (12', 16'). A ce titre, il existe une relation logique entre le dernier processus d'authentification d'entité et les clés de chiffrement (70) générées consécutivement. La sécurité s'en trouve renforcée et cela permet de réduire le traitement et les délais de surcharge associés à la répétition de la liaison ou du processus d'authentification d'entité. Ces procédés et ces dispositifs peuvent servir à améliorer la sécurité dans n'importe quel système de communication, y compris un système de télécommunication mobile, tel qu'un système GSM.

## Classes/Indexing

### IPC

IPC Code(1-7) **H04L 9/32**

(7)

Current IPC-R	Invention	Version	Additional	Version
Advanced	H04L 9/08	20060101	-	-
	H04L 9/32	20060101		
	H04Q 7/38	20060101		
Core	H04L 9/08	20060101	-	-
	H04L 9/32	20060101		
	H04Q 7/38	20060101		
Subclass	-	-	-	-

Original IPC-R	Invention	Version	Additional	Version
Advanced	H04L 9/32	20060101	-	-
Core	H04L 9/32	20060101	-	-
Subclass	-	-	-	-

### ECLA

H04L000932R

### DWPI Manual Codes

Expand DWPI Manual Codes

## Legal Status

### INPADOC Legal Status

Gazette Date	Code	Description
2004-07-07	18D -	DEEMED TO BE WITHDRAWN 2004-01-03
2004-05-06	RAP1	TRANSFER OF RIGHTS OF AN EP APPLICATION TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)
2002-03-27	AK +	DESIGNATED CONTRACTING STATES: EP 1190526 A1 AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
2002-03-27	17P +	REQUEST FOR EXAMINATION FILED 2002-01-16
2002-03-27	AX +	EXTENSION OF THE EUROPEAN PATENT TO AL LT LV MK RO SI

Get Family Legal Status

### EPO License

Expand License

### EPO Procedural Status

Expand EPO Procedural Status

## Family

### Family

Expand INPADOC Family (7)

## Claims

No Claims exist for this Record

## Description

### Description

 Expand Description

## Citations

### Citation

Citing Patents (0)

Cited Patents (0)

 Expand Cited Non-patents (1)

## Other

### Attorney / Agent

O'Connell, David Christopher

### PCT Application / Publication

WO2000EP5742A / 2000-06-21  
WO2001001630A1 / 2001-01-04

### Designated States

**European patent:** AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

Copyright 2007-2010 THOMSON REUTERS